Opportunistic relaying and random linear network coding for secure and reliable communication

Amjad Saeed Khan, *Student Member, IEEE* and Ioannis Chatzigeorgiou, *Senior Member, IEEE*

***Abstract*—Opportunistic relaying has the potential to achieve full diversity gain, while random linear network coding (RLNC) can reduce latency and energy consumption. In recent years, there has been a growing interest in the integration of both schemes into wireless networks in order to reap their benefits while taking into account security concerns. This paper considers a multi-relay network, where relay nodes employ RLNC to encode confidential data and transmit coded packets to a destination in the presence of an eavesdropper. Four relay selection protocols are studied covering a range of network capabilities, such as the availability of the eavesdropper's channel state information or the possibility to pair the selected relay with a node that intentionally generates interference. For each case, expressions for the probability that a coded packet will not be recovered by a receiver, which can be either the destination or the eavesdropper, are derived. Based on those expressions, a framework is developed that characterizes the probability of the eavesdropper intercepting a sufficient number of coded packets and partially or fully recovering the confidential data. Simulation results confirm the validity and accuracy of the theoretical framework and unveil the security-reliability trade-offs attained by each RLNC-enabled relay selection protocol.**

***Index Terms*—Relay selection, random linear network coding, physical-layer security, outage probability, intercept probability.**

I. Introduction

The dynamic nature of the wireless medium often introduces problems to the operation of wireless networks, which are related to node connectivity, communication reliability and robustness [1]. Methods that can ameliorate the side effects of wireless environments include *opportunistic relaying* and *node cooperation* [2]. For example, opportunistic relaying was proposed as an alternative to distributed space-time relaying; it achieves full diversity gain [3] but can also improve energy efficiency [4], [5]. Opportunistic routing based on cooperative forwarding was presented in [6] to combat errors and link failures in sensor networks. Multi-phase node cooperation for indoor industrial monitoring was described in [7] as a means to reduce energy consumption. Moreover, an experimental study of selective cooperative relaying was provided in [8].

In energy-constraint wireless networks, such as sensor networks, the communicating nodes are typically battery powered and have a limited energy budget. The improvement of the network lifetime without a reduction in network reliability is a major challenge. *Random Linear Network Coding* (RLNC) can decrease the number of distinct packet transmissions in a network and minimize or eliminate packet retransmissions due to poor channel conditions [9]. Consequently, RLNC has the potential to both improve energy efficiency [10] and reduce the overall latency in a network [11], which effectively lead to an increase in the lifetime of the network. The key idea behind RLNC is that nodes are allowed to linearly combine stored data packets and generate coded packets, rather than simply store and forward data packets. Advantages from using opportunistic relaying with network coding in two-way relay communications have been reported in [12]–[14].

Even though opportunistic relaying and RLNC have the potential to improve energy efficiency and link reliability, the broadcast nature of the wireless medium renders data transmission to an authorized destination vulnerable to eavesdropping. The secure delivery of confidential data is important for many applications, for example, sharing of sensitive information or key distribution. *Physical-layer security* (PLS) is a promising method that complements existing cryptographic techniques and can be easily integrated into wireless networks that combine opportunistic relaying with cooperative communication [15]–[17]. In [15], a relay selection metric that utilizes knowledge of the relay-to-eavesdropper instantaneous channel conditions was presented and the network performance was evaluated in terms of the secrecy outage probability. Opportunistic relay selection protocols in the presence of multiple eavesdroppers were studied in [16]. The effect of single-relay and multi-relay selection on the performance of physical layer security in wireless networks was investigated in [17] and security-reliability tradeoffs were identified using comparisons between the intercept probability and the outage probability of direct transmission. *Cooperative jamming* has been proposed as a means to further enhance PLS by selecting a node that will generate intentional inference with the aim of degrading the quality of an eavesdropper's channel. For example, joint relay-and-jammer selection techniques were proposed in [18] to increase the secrecy capacity in wireless networks, whereas suboptimal relay selection and suboptimal joint relay-and-jammer selection protocols were compared in [19].

The main objective of PLS techniques is to increase the secrecy rate between the source and the destination, while ensuring that the transmitted information cannot be accessed by an eavesdropper. Strict information-theoretic security is achieved if and only if the mutual information between the packets available to an eavesdropper and the source packets is zero [20]. The performance of PLS schemes is often measured by the *secrecy capacity*, which is the maximum rate for reliable and perfectly secure communication, and the *secrecy outage*

This work was supported by the Royal Society International Exchanges Scheme under grant IE140855.

A. S. Khan and I. Chatzigeorgiou are with the School of Computing and Communications, Lancaster University, Lancaster, United Kingdom (e-mail: {a.khan9, i.chatzigeorgiou}@lancaster.ac.uk).

probability, which is the probability that secure communication will fail. However, these two metrics are used to optimize the transmission rate, so that the legitimate destination will fully recover the transmitted data with perfect secrecy. If information-theoretic secrecy cannot be achieved, the secrecy capacity and the secrecy outage probability do not provide any insight into the likelihood of an eavesdropper recovering only a *fraction* of the transmitted confidential information.

To the best of our knowledge, only few studies that exploit the properties of RLNC in PLS are available. For example, the intrinsic nature of RLNC against eavesdropping attacks was analysed in [21] and the advantages of feedback-based transmissions were identified. To enhance the secrecy of cooperative transmissions in sensor networks, fountain-coding aided cooperative relaying with jamming was proposed in [22]. In contrast to [22], where only one relay has been considered for aiding the source in its transmission to the destination, we consider the complete problem of selecting a relay or a relay-jammer pair from the set of available nodes. Furthermore, relays do not only perform decode-and-forward, as in [22], but also linearly combine recovered data packets. In other words, relays employ random linear fountain coding, which can be seen as an implementation of RLNC for broadcast communication. Other notable differences from [22] include the derivation of the probability that a fraction of data will leak to the eavesdropper, as opposed to the total amount of transmitted data, and the investigation of the impact of both the finite field size used by RLNC and the adopted forward error correction and modulation scheme on the security and reliability of the network.

The motivation for this paper is to investigate the potential of relay-aided networks that combine RLNC with opportunistic relaying, with or without cooperative jamming, in securely and reliably delivering confidential messages. To this end, we consider four different relay selection protocols, we analyze their outage behavior and we quantify the proportion of the message that could leak to the eavesdropper with a certain probability by the time the legitimate destination has recovered the entire message with a target probability. The main contributions of the paper can be summarized as follows:

1) We propose a cross-layer security scheme, which combines the inherent secrecy features of RLNC at the application layer with physical-layer security mechanisms, based on relay selection with or without jamming.
2) We derive analytical expressions of the outage probability at the destination and the eavesdropper. SNR thresholds that characterize the modulation and coding scheme at the physical layer have been used, so that the outage probability can be linked to the packet error probability in the case of Rayleigh frequency-flat fading channels.
3) We introduce a novel leakage metric, which is referred to as the $\tau-$intercept probability and is defined as the probability that a proportion of the transmitted information will be compromised. An exact expression of the τ-intercept probability is derived for systems that impose a deadline on coded packet transmissions but provide the destination with a feedback link, which can be used to terminate the transmission process before the deadline expires.
4) We investigate the secrecy-reliability trade-offs of the considered RLNC-enabled relay selection protocols.

The rest of the paper is organized as follows. Section II describes the system model and introduces the relevant notation. A detailed description of the relay selection protocols is provided in Section III and outage probability expressions for both the destination and the eavesdropper are derived. The equivalence between the outage probability and the packet error probability is exploited in Section IV and an exact expression of the τ-intercept probability for RLNC-enabled opportunistic relaying is derived. Results are discussed in Section V and conclusions are drawn in Section VI.

II. System Model

As shown in Fig. 1, we consider a network that consists of a source S, a destination D and a set of N trusted nodes $\mathcal{S}_N = \{1, \ldots, N\}$. The source could be an independent node or an element of $\mathcal{S}_N$. The main objective of the nodes in $\mathcal{S}_N$ is to relay information from the source to the destination. However, they can also cause interference to overhearing attacks by an eavesdropper, denoted by E. Links between the source and the destination as well as between the source and the eavesdropper are not considered; the direct links could be in deep shadowing or the destination and the eavesdropper could be outside the coverage area of the source. This is an assumption that is often made in the context of cooperative communications [23], [24], as well as in cooperative relaying for secure communications [19], [25], [26].

A centralized network topology has been used, whereby a control unit located in the source S or a dedicated controller node employs one of the following protocols in order to select a single node or a pair of nodes:

1) *Conventional selection*: Similarly to [15], the relay that provides the best instantaneous relay-to-destination channel quality is selected.
2) *Optimal selection*: Selection of the optimal relay considers the instantaneous channel quality of both links that originate from each candidate node and terminate at the destination and the eavesdropper, respectively [15].
3) *Conventional selection with jammer*: The conventional selection protocol is first used to determine the node that will act as a relay. The worst instantaneous relay-to-destination link is then identified to determine the node that will transmit noise concurrently with the chosen relay in an effort to degrade the reception quality at the eavesdropper while causing the least interference for the destination.
4) *Optimal selection with preset jammer*: In this case, the node that acts as a jammer is fixed, while the node that acts as a relay is chosen from the remaining nodes in $\mathcal{S}_N$ using the optimal selection protocol.

The relay selected by each of the four protocols is denoted by n^*, the jammer selected by the third protocol in the list is represented by J^*, and the preset jammer in the last protocol is denoted by J. We have opted for optimal selection with a preset jammer in order to provide some insight into how the reliability and security offered by optimal relaying is affected

by the introduction of a jammer. Specific techniques for the selection of the appropriate jammer that could further improve the secrecy performance of the network at the expense of reliability could be considered [18], [27] but this discussion is beyond the scope of this paper.

In order to fully exploit spatial diversity, our analysis assumes that the control unit has knowledge of the channel state information (CSI) at the destination in all four protocols. The control unit also has knowledge of the CSI at the eavesdropper in the case of optimal selection with or without a jammer. Note that this is a common assumption in the physical-layer security literature [16], [28]. For example, the eavesdropper's CSI can be known if the eavesdropper is part of the network of legitimate receivers when unclassified data are broadcast, but is treated as an unauthorized receiver when confidential data are transmitted. Even if an eavesdropper is never destined to receive any type of transmitted data, its presence can still be detected from power leaked via its antenna port while in receiving mode [29].

The delivery of a confidential message by the source to the destination using opportunistic relaying is divided into two phases. In the *first phase*, the source broadcasts the message and the candidate relay nodes operate in receiving mode. This paper studies the impact that the RLNC-enabled relay selection schemes have on the leakage and reliability of information broadcast from the relay nodes. For this reason, we assume that at the end of the first phase all of the relays have successfully recovered the message. For example, the source could employ RLNC to segment the message into multiple packets and encode them. The source would then broadcast randomly generated coded packets until all receiving nodes in $\mathcal{S}_N$ have reconstructed the message. Alternatively, the source could transmit coded packets until one of the nodes in $\mathcal{S}_N$ has recovered the message; the nodes in $\mathcal{S}_N$ could then use short-range communication to exchange packets until all nodes have knowledge of the message. In the *second phase*, each node in $\mathcal{S}_N$ divides the message into K data packets. Based on the adopted relay selection protocol, the control unit instructs the chosen relay n^* to employ RLNC on the data packets and generate a coded packet. The coded packet is further processed by the transmission scheme at the physical layer of the relay. The transmission scheme, which involves forward error correction and modulation techniques, can be accurately characterized by a signal-to-noise ratio (SNR) threshold, denoted by $\gamma_{\rm th}$, as described in [30]–[32]. This process is repeated up to $N_{\rm T}$ times and, thus, up to $N_{\rm T}$ coded packets are transmitted; each time, the appropriate relay is selected from $\mathcal{S}_N$, depending on the instantaneous channel conditions. Both the destination D and the eavesdropper E collect coded packets and use them to construct local decoding matrices. If K linearly independent coded packets are received, the rank of the decoding matrix will be K. This implies that the K data packets can be recovered and the entire message can be reconstructed. If the destination recovers the message before the set deadline of $N_{\rm T}$ transmissions, it sends a notification to the control unit to terminate the relay selection and packet transmission process.

The relay-to-destination links and the relay-to-eavesdropper links have been modeled as independent but not identically distributed (i.n.i.d) quasi-static Rayleigh fading channels [18]. The channel gain between nodes i and j, denoted by $|h_{i,j}|$, remains constant for the duration of a coded packet but changes independently from packet to packet. The variance of the fading distribution is given by $\sigma_{i,j}^2 = \mathbb{E}\left\{|h_{i,j}|^2\right\} = d_{i,j}^{-\alpha_{i,j}}$, where $\mathbb{E}\left\{|h_{i,j}|^2\right\}$ represents the expected value of $|h_{i,j}|^2$, and $d_{i,j}$ and $\alpha_{i,j}$ are the Euclidean distance and the path loss exponent between the two nodes, respectively. Furthermore, links are impaired by additive white Gaussian noise with zero mean and variance N_0. The instantaneous SNR of the link between i and j is represented as $\gamma_{i,j} = P_i|h_{i,j}|^2/N_0$, where P_i is the transmitted power of node i. The probability density function of $\gamma_{i,j}$ is equal to [33]

$$f_{\gamma_{i,j}}(\gamma) = \Pr(\gamma_{i,j} = \gamma) = \lambda_{i,j} e^{-\gamma\lambda_{i,j}} \tag{1}$$

where $\lambda_{i,j} = 1/\mathbb{E}\left\{\gamma_{i,j}\right\}$. The cumulative density function of $\gamma_{i,j}$ can be obtained as follows

$$F_{\gamma_{i,j}}(\gamma_{\rm th}) = \Pr(\gamma_{i,j} \le \gamma_{\rm th}) = 1 - e^{-\gamma_{\rm th}\lambda_{i,j}}. \tag{2}$$

For convenience, the key parameters of the system model have been summarized in Table I.

Table I
KEY PARAMETERS OF THE SYSTEM MODEL

Notation	Description
K	Number of data packets.
N	Number of relay nodes.
$\mathcal{S}_N$	Set of N trusted relay nodes.
P_i	Transmitted power of node i.
N_0	Variance of the additive white Gaussian noise
$h_{i,j}$	Fading coefficient of the channel between nodes i and j.
$\gamma_{i,j}$	Instantaneous SNR of the link between nodes i and j.
$\lambda_{i,j}$	The inverse of the average SNR of the link between nodes i and j.
$\gamma_{\rm th}$	Required SNR threshold for signal recovery at the receiving node $u \in \{\mathrm{D}, \mathrm{E}\}$.
$\rho_{\rm u}$	Outage probability at node u, where $u \in \{\mathrm{D}, \mathrm{E}\}$.
n^*	Selected relay.
J^*	Selected jammer.
J	Preset jammer.
$n_{\rm T}$	Number of transmitted coded packets.
$n_{\rm R}$	Number of received coded packets.
$N_{\rm T}$	Maximum permitted number of coded packet transmissions.

Both the destination and the eavesdropper in the considered system model apply the Gaussian elimination method on their respective decoding matrices to compute their rank and recover the source message. The objective of the destination is to recover the entire message, i.e., all of the K data packets. Traditionally, the communication process is deemed to be secure if the eavesdropper fails to recover the message [21], [34]. By contrast, this paper assumes that the probability of the eavesdropper decoding the received coded packets and recovering even a subset of the K data packets should be very small. We shall refer to the probability of the eavesdropper retrieving at least τ of the K data packets as τ-intercept probability and we will evaluate it in Section IV. However, we will first investigate the impact of the considered relay

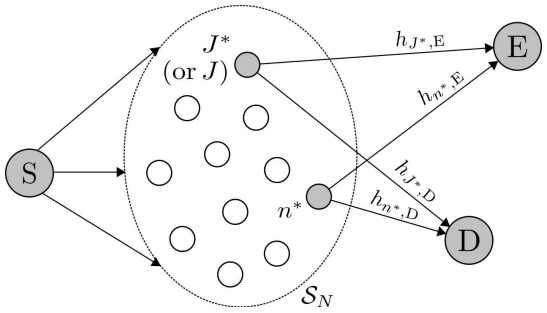

Figure 1. Block diagram of the system model.

selection protocols on the capability of the system to reliably and securely relay confidential messages in Section III.

III. Relay Selection and Outage Analysis

This section describes the relay selection protocols in greater detail, and characterizes their performance in terms of the outage probability at the destination D and the outage probability at the eavesdropper E. The outage probability is the probability that the instantaneous signal-to-interference-plus-noise ratio (SINR) at a receiving node, either D or E, will drop below a predefined threshold γ_{th} due to an event, e.g., deep fading or interference. The outage probability at the destination D and the eavesdropper E, denoted by ρ_{D} and ρ_{E}, respectively, can be expressed as:

$$\rho_{\mathrm{D}} = \Pr(\mathrm{SINR}_{n^*,\mathrm{D}} \leq \gamma_{\mathrm{th}})$$
$$\rho_{\mathrm{E}} = \Pr(\mathrm{SINR}_{n^*,\mathrm{E}} \leq \gamma_{\mathrm{th}})$$

where n^* represents the selected relay. As established in [30] for Rayleigh fading channels and extended in [31] and [32] for other channel models, the outage probability is a very tight approximation of the packet error probability, if the value of γ_{th} accurately reflects the employed modulation and coding scheme. For example, $\gamma_{\mathrm{th}} = 5.89$ dB for uncoded BPSK and $\gamma_{\mathrm{th}} = -0.983$ dB for BPSK combined with a typical convolutional code [30] over Rayleigh fading channels. Analytical expressions of ρ_{D} and ρ_{E} are derived in this section, which first considers the protocols that only use opportunistic relaying and then focuses on the protocols that combine relaying with jamming.

A. Relay Selection Protocols without Jammer

1) Conventional selection: This protocol only considers the channel quality of the relay-to-destination link. A relay n^* is selected from $\mathcal{S}_N$, such that

$$n^* = \arg\max_{n \in \mathcal{S}_N} \gamma_{n,\mathrm{D}}.$$

Owing to the fact that no interference is introduced by a jammer, the SINR at the destination D and the SINR at the eavesdropper E are $\mathrm{SINR}_{n^*,\mathrm{D}} = \gamma_{n^*,\mathrm{D}}$ and $\mathrm{SINR}_{n^*,\mathrm{E}} = \gamma_{n^*,\mathrm{E}}$, respectively. The outage probability ρ_{D} can be obtained by considering the joint probability of every node in $\mathcal{S}_N$ being the selected relay and its link being in outage, that is,

$$\rho_{\mathrm{D}} = \sum_{n=1}^{N} \Pr\left[(n^* = n) \bigcap (\gamma_{n,\mathrm{D}} \leq \gamma_{\mathrm{th}})\right]. \tag{3}$$

If we take into account that the channels are statistically independent and that $\gamma_{n,\mathrm{D}}$ follows the distribution given in (1), we can use order statistics [35] and obtain:

$$\begin{aligned}\Pr(n^* = n) &= \int_0^\infty \prod_{i=1, i\neq n}^{N} \Pr(\gamma_{i,\mathrm{D}} \leq x) f_{\gamma_{n,\mathrm{D}}}(x)\, dx \\ &= \int_0^\infty \prod_{i=1, i\neq n}^{N} \left(1 - e^{-x\lambda_{i,\mathrm{D}}}\right) f_{\gamma_{n,\mathrm{D}}}(x)\, dx.\end{aligned} \tag{4}$$

The joint probability in (3) can be obtained from (4) by setting the upper limit of the integral in (4) to γ_{th}, resulting in:

$$\rho_{\mathrm{D}} = \sum_{n=1}^{N} \int_0^{\gamma_{\mathrm{th}}} \prod_{i\neq n}^{N} \left(1 - e^{-x\lambda_{i,\mathrm{D}}}\right) f_{\gamma_{n,\mathrm{D}}}(x)\, dx. \tag{5}$$

Using the multinomial identity [36], the product of terms in (5) can be expanded as follows:

$$\prod_{i\neq n}^{N} (1 - e^{-x\lambda_{i,\mathrm{D}}}) = \sum_{m=0}^{N-1} \sum_{\substack{\mathcal{S}_m \subseteq \mathcal{S}_N \setminus n \\ |\mathcal{S}_m| = m}} (-1)^m e^{-x \sum_{i\in\mathcal{S}_m} \lambda_{i,\mathrm{D}}} \tag{6}$$

where the inner sum in (6) is over all possible sets $\mathcal{S}_m$ of size m that are subsets of $\mathcal{S}_N$ but exclude the node n. Substituting (6) into (5) and solving the integral leads to:

$$\rho_{\mathrm{D}} = \sum_{n=1}^{N} \sum_{m=0}^{N-1} \sum_{\substack{\mathcal{S}_m \subseteq \mathcal{S}_N \setminus n \\ |\mathcal{S}_m| = m}} (-1)^m \frac{\lambda_{n,\mathrm{D}}}{\sum_{i\in\mathcal{S}_m} \lambda_{i,\mathrm{D}} + \lambda_{n,\mathrm{D}}} \left[1 - e^{-\gamma_{\mathrm{th}}(\sum_{i\in\mathcal{S}_m} \lambda_{i,\mathrm{D}} + \lambda_{n,\mathrm{D}})}\right].$$

Following the same line of thought, the outage probability at the eavesdropper E can be obtained as follows:

$$\rho_{\mathrm{E}} = \sum_{n=1}^{N} \Pr(n^* = n) \Pr(\gamma_{n,\mathrm{E}} \leq \gamma_{\mathrm{th}}) \tag{7}$$

because $\gamma_{n,\mathrm{D}}$, which determines $\Pr(n^* = n)$ is independent of $\gamma_{n,\mathrm{E}}$. Based on (2), we have

$$Pr(\gamma_{n,\mathrm{E}} \leq \gamma_{\mathrm{th}}) = 1 - e^{-\gamma_{\mathrm{th}}\lambda_{n,\mathrm{E}}}$$

therefore, expression (7) assumes the form:

$$\rho_{\mathrm{E}} = \sum_{n=1}^{N} \int_0^\infty \prod_{i\neq n,}^{N} \left(1 - e^{-x\lambda_{i,\mathrm{D}}}\right)\left(1 - e^{-\gamma_{\mathrm{th}}\lambda_{n,\mathrm{E}}}\right) dx.$$

Invoking (6) and solving the integral gives the following closed form expression:

$$\rho_{\mathrm{E}} = \sum_{n=1}^{N} \sum_{m=0}^{N-1} \sum_{\substack{\mathcal{S}_m \subseteq \mathcal{S}_N \setminus n \\ |\mathcal{S}_m| = m}} (-1)^m \frac{\lambda_{n,\mathrm{D}}}{\sum_{i\in\mathcal{S}_m} \lambda_{i,\mathrm{D}} + \lambda_{n,\mathrm{D}}} \left(1 - e^{-\gamma_{\mathrm{th}}\lambda_{n,\mathrm{E}}}\right).$$

2) Optimal selection: This protocol is deemed 'optimal' because it exploits knowledge of the eavesdropper's CSI and achieves the maximum secrecy capacity [18]. For this reason, this paper uses optimal selection as a benchmark protocol and compares its performance to that of the other three protocols. According to this protocol, the relay n^* is selected such that

$$n^* = \arg\max_{n \in \mathcal{S}_N} \left(\frac{\gamma_{n,\mathrm{D}}}{\gamma_{n,\mathrm{E}}}\right).$$

The outage probability at the destination can be obtained from the general expression (3) if the probability of the selected relay being a particular node is expressed as:

$$\Pr(n^*=n)=\int_0^\infty\int_0^\infty I_1(x,y)f_{\gamma_{n,\mathrm{D}}}(x)f_{\gamma_{n,\mathrm{E}}}(y)\,dx\,dy \quad (8)$$

where

$$I_1(x,y)=\prod_{\substack{i=1\\ i\neq n}}^{N}\Pr\left(\frac{\gamma_{i,\mathrm{D}}}{\gamma_{i,\mathrm{E}}}\leq\frac{x}{y}\right). \quad (9)$$

If we set $\Lambda_i=\frac{\lambda_{i,\mathrm{D}}}{\lambda_{i,\mathrm{E}}}$, expression (9) can be rewritten as [16]:

$$I_1(x,y)=\prod_{\substack{i=1\\ i\neq n}}^{N}\frac{x\Lambda_i}{x\Lambda_i+y}. \quad (10)$$

Using partial fraction expansion and simplifying the resultant expression, (10) assumes the form:

$$I_1(x,y)=1-\sum_{\substack{i=1\\ i\neq n}}^{N}\frac{y\Theta_i}{x\Lambda_i+y}$$

where Θ_i is the partial fraction coefficient and is equal to:

$$\Theta_i=\prod_{k\notin\{n,i\}}\frac{-\Lambda_k}{\Lambda_i-\Lambda_k},\quad \text{for}\,\Lambda_k\neq\Lambda_i.$$

Substituting (8) into (3) and taking into account that $\gamma_{n,\mathrm{D}}$ should not exceed γ_{th} gives:

$$\rho_{\mathrm{D}}=\sum_{n=1}^{N}\int_0^\infty\int_0^{\gamma_{\mathrm{th}}} I_1(x,y)f_{\gamma_{n,\mathrm{D}}}(x)f_{\gamma_{n,\mathrm{E}}}(y)\,dx\,dy.$$

Invoking [37, eq. (3.352.1)] and the relationships in [38, Section 4.2], we obtain:

$$\begin{aligned}\rho_{\mathrm{D}}=&\sum_{n=1}^{N}1-e^{-\gamma_{\mathrm{th}}\lambda_{n,\mathrm{D}}}+\sum_{j\neq n}\Theta_j\lambda_{n,\mathrm{E}}e^{-\gamma_{\mathrm{th}}(\lambda_{n,\mathrm{D}}-\Lambda_j\lambda_{n,\mathrm{E}})}\\ &\left[\mathrm{E}_1\big((\alpha_2+1)\lambda_{n,\mathrm{D}}\gamma_{\mathrm{th}}\big)\left\{\frac{\Lambda_j\gamma_{\mathrm{th}}}{\alpha_2}-\frac{\Lambda_j}{\lambda_{n,\mathrm{D}}\alpha_2^2}\right\}+e^{-\gamma_{\mathrm{th}}\alpha_2\lambda_{n,\mathrm{D}}}\right.\\ &\left.\mathrm{E}_1(\gamma_{\mathrm{th}}\lambda_{n,\mathrm{D}})\frac{\Lambda_j}{\lambda_{n,\mathrm{D}}\alpha_2^2}-\frac{\Lambda_j}{\lambda_{n,\mathrm{D}}\alpha_2(\alpha_2+1)}e^{-\gamma_{\mathrm{th}}(\alpha_2+1)\lambda_{n,\mathrm{D}}}\right]\\ &-\frac{\Theta_j\lambda_{n,\mathrm{D}}\lambda_{n,\mathrm{E}}}{\Lambda_j\alpha_1^2}\left\{\ln\left(1+\frac{\alpha_1}{\beta_1}\right)-\frac{\alpha_1}{\lambda_{n,\mathrm{E}}}\right\}\end{aligned} \quad (11)$$

where $\alpha_1=\lambda_{n,\mathrm{E}}-\frac{\lambda_{n,\mathrm{D}}}{\Lambda_j}$, $\alpha_2=\frac{\Lambda_j\lambda_{n,\mathrm{E}}}{\lambda_{n,\mathrm{D}}}-1$, $\beta_1=\frac{\lambda_{n,\mathrm{D}}}{\Lambda_j}$ and E_1 is the exponential integral, as defined in [37].

The value of $\gamma_{n,\mathrm{E}}$ in optimal relay selection affects the probability that a node will be selected to act as a relay. As a result, and in contrast to (7), the outage probability at the eavesdropper has to be expressed as the summation of joint probabilities, as follows:

$$\rho_{\mathrm{E}}=\sum_{n=1}^{N}\Pr\left[(n^*=n)\bigcap(\gamma_{n,\mathrm{E}}\leq\gamma_{\mathrm{th}})\right].$$

Taking into account (8) and recalling that the value of $\gamma_{n,\mathrm{E}}$ needs to be upper bounded by γ_{th}, we obtain:

$$\rho_{\mathrm{E}}=\sum_{n=1}^{N}\int_0^{\gamma_{\mathrm{th}}}\int_0^\infty I_1(x,y)f_{\gamma_{n,\mathrm{D}}}(x)f_{\gamma_{n,\mathrm{E}}}(y)\,dx\,dy.$$

Derivation of an analytical expression for ρ_{E} requires a similar approach to that in (11), and leads to:

$$\begin{aligned}\rho_{\mathrm{E}}=&\sum_{n=1}^{N}1-e^{-\gamma_{\mathrm{th}}\lambda_{n,\mathrm{E}}}+\sum_{j\neq n}\frac{\Theta_j\lambda_{n,\mathrm{D}}\lambda_{n,\mathrm{E}}}{\Lambda_j\alpha_1^2}\Big[\mathrm{E}_1\big(\lambda_{n,\mathrm{E}}\gamma_{\mathrm{th}}\big)-(1+\alpha_1\gamma_{\mathrm{th}})\cdot\\ &\cdot e^{-\alpha_1\gamma_{\mathrm{th}}}\mathrm{E}_1(\beta_1\gamma_{\mathrm{th}})-\frac{\alpha_1}{\lambda_{n,\mathrm{E}}}\big(1-e^{-\gamma_{\mathrm{th}}\lambda_{n,\mathrm{E}}}\big)+\ln\left(1+\frac{\alpha_1}{\beta_1}\right)\Big].\end{aligned}$$

B. Relay Selection Protocols with Jammer

In an effort to increase the outage probability at the eavesdropper, a jammer can be employed by the two aforementioned protocols. The selection mechanism of the jammer and its impact on the outage probability at the destination and at the eavesdropper are investigated in this subsection.

1) Conventional selection with jammer: This protocol is based on a joint relay-jammer pair selection scheme. Similarly to conventional selection, this protocol first selects a relay n^* from $\mathcal{S}_N$ that provides the best instantaneous SNR at the destination. Subsequently, one of the remaining nodes in $\mathcal{S}_N$ is selected to act as a jammer, such that it causes the least interference to the destination. The pair selection scheme can be described by the following expressions:

$$n^*=\arg\max_{n\in\mathcal{S}_N}\gamma_{n,\mathrm{D}}$$

$$J^*=\arg\min_{j\in\mathcal{S}_N\setminus n^*}\gamma_{j,\mathrm{D}}.$$

The SINR at the destination and the SINR at the eavesdropper are given by

$$\mathrm{SINR}_{n^*,\mathrm{D}}=\frac{\gamma_{n^*,\mathrm{D}}}{\gamma_{J^*,\mathrm{D}}+1}$$

$$\mathrm{SINR}_{n^*,\mathrm{E}}=\frac{\gamma_{n^*,\mathrm{E}}}{\gamma_{J^*,\mathrm{E}}+1}.$$

repectively. Clearly, both $\mathrm{SINR}_{n^*,\mathrm{D}}$ and $\mathrm{SINR}_{n^*,\mathrm{E}}$ depend on the selected nodes n^* and J^*.

The outage probability at the destination should consider the joint probability of a node n being the relay, a different node m being the jammer, and the SINR at the destination not exceeding the SNR threshold γ_{th}, for all possible values of n and m. Therefore, ρ_{D} can be written as:

$$\rho_{\mathrm{D}}=\sum_{n=1}^{N}\sum_{m\neq n}^{N}\Pr\left[(n^*=n)\bigcap(J^*=m)\bigcap\left(\frac{\gamma_{n,\mathrm{D}}}{\gamma_{m,\mathrm{D}}+1}\leq\gamma_{\mathrm{th}}\right)\right]. \quad (12)$$

Taking into account that the instantaneous SNR of the jammer-to-destination channel cannot be greater than the instantaneous SNR of the relay-to-destination channel, and that the two channels are independent, we can express the joint probability of selecting a relay-jammer pair as follows:

$$\Pr\Big[(n^*=n)\bigcap(J^*=m)\Big]=\int_0^\infty\int_0^{\gamma_{n,\mathrm{D}}} I_2(x,y)f_{\gamma_{m,\mathrm{D}}}(y)f_{\gamma_{n,\mathrm{D}}}(x)\,dy\,dx \quad (13)$$

where

$$I_2(x,y)=\prod_{i\neq n, i\neq m}^{N-2}\Pr(y\leq\gamma_{i,\mathrm{D}}\leq x).$$

Invoking (2), $I_2(x,y)$ assumes the form:

$$I_2(x,y)=\prod_{i\neq n, i\neq m}^{N-2}\left(e^{-y\lambda_{i,\mathrm{D}}}-e^{-x\lambda_{i,\mathrm{D}}}\right)$$

which can be rewritten as:

$$I_2(x,y)=\sum_{w=0}^{N-2}\sum_{\substack{\mathcal{X}=\mathcal{S}_N\setminus\{n,m\}\\ \mathcal{S}_w\subseteq\mathcal{X},\bar{\mathcal{S}}_w\subseteq\mathcal{X}\\ |\mathcal{S}_w|=w}}(-1)^w e^{-x\sum_{i\in\mathcal{S}_w}\lambda_{i,\mathrm{D}}-y\sum_{j\in\bar{\mathcal{S}}_w}\lambda_{j,\mathrm{D}}}$$

using the multinomial identity. Substituting (13) into (12) and properly setting the limits of the two integrals gives:

$$\rho_{\mathrm{D}}=\sum_{n=1}^{N}\sum_{m\neq n}^{N}\int_0^{\delta}\int_y^{(y+1)\gamma_{\mathrm{th}}}I_2(x,y)f_{\gamma_{n,\mathrm{D}}}(x)f_{\gamma_{m,\mathrm{D}}}(y)\,dx\,dy$$

where $\delta=\infty$ for $\gamma_{\mathrm{th}}\geq 1$, and $\delta=\frac{\gamma_{\mathrm{th}}}{1-\gamma_{\mathrm{th}}}$ otherwise. Solving the integrals, we obtain:

$$\rho_{\mathrm{D}}=\sum_{n=1}^{N}\sum_{m\neq n}^{N}\sum_{w=0}^{N-2}\sum_{\substack{\mathcal{X}=\mathcal{S}_N\setminus\{n,m\}\\ \mathcal{S}_w\subseteq\mathcal{X},\bar{\mathcal{S}}_w\subseteq\mathcal{X}\\ |\mathcal{S}_w|=w}}(-1)^w\lambda_{n,\mathrm{D}}\,\lambda_{m,\mathrm{D}}\,\delta_{n,m}$$

where

$$\delta_{n,m}=\begin{cases}\dfrac{1}{c_n\lambda_{\mathrm{D}}}-\dfrac{e^{-\gamma_{\mathrm{th}}c_n}}{c_n c_{n,m}}, & \text{for } \gamma_{\mathrm{th}}\geq 1\\ \dfrac{1-e^{-\frac{\gamma_{\mathrm{th}}\lambda_{\mathrm{D}}}{1-\gamma_{\mathrm{th}}}}}{c_n\lambda_{\mathrm{D}}}-e^{\gamma_{\mathrm{th}}c_n}\left[\dfrac{1-e^{-\frac{\gamma_{\mathrm{th}}c_{n,m}}{1-\gamma_{\mathrm{th}}}}}{c_n c_{n,m}}\right], & \text{for } \gamma_{\mathrm{th}}<1\end{cases}$$

and $c_n=\left(\sum_{i\in\mathcal{S}_w}\lambda_{i,\mathrm{D}}+\lambda_{n,\mathrm{D}}\right)$, $c_m=\left(\sum_{j\in\bar{\mathcal{S}}_w}\lambda_{j,\mathrm{D}}+\lambda_{m,\mathrm{D}}\right)$, $c_{n,m}=(\gamma_{\mathrm{th}}c_n+c_m)$, $\lambda_{\mathrm{D}}=\sum_{k=1}^{N}\lambda_{k,\mathrm{D}}$.

Due to the fact that the process of selecting the relay and the jammer is independent of the eavesdropper's CSI, the outage probability at the eavesdropper can be obtained as follows:

$$\rho_{\mathrm{E}}=\sum_{n=1}^{N}\sum_{m\neq n}^{N}\Pr\Big[(n^*=n)\bigcap(J^*=m)\Big]\Pr\left(\frac{\gamma_{n,\mathrm{E}}}{\gamma_{m,\mathrm{E}}+1}\leq\gamma_{\mathrm{th}}\right).$$

Using (13), we can express the joint probability of selecting the relay-jammer pair as:

$$\Pr\Big[(n^*=n)\bigcap(J^*=m)\Big]=\sum_{w=0}^{N-2}\sum_{\substack{\mathcal{X}=\mathcal{S}_N\setminus\{n,m\}\\ \mathcal{S}_w\subseteq\mathcal{X},\bar{\mathcal{S}}_w\subseteq\mathcal{X}\\ |\mathcal{S}_w|=w}}(-1)^w\frac{\lambda_{n,\mathrm{D}}\lambda_{m,\mathrm{D}}}{c_m}\left[\frac{1}{c_n}-\frac{1}{\lambda_{\mathrm{D}}}\right]$$

while the probability that the SINR at the eavesdropper will not be greater than the SNR threshold is given by

$$\begin{aligned}\Pr\left(\frac{\gamma_{n,\mathrm{E}}}{\gamma_{m,\mathrm{E}}+1}\leq\gamma_{\mathrm{th}}\right)&=\Pr\big(\gamma_{n,\mathrm{E}}\leq\gamma_{\mathrm{th}}(\gamma_{m,\mathrm{E}}+1)\big)\\&=\int_0^{\infty}\left(1-e^{-\gamma_{\mathrm{th}}(y+1)}\right)f_{\gamma_{m,\mathrm{E}}}(y)\,dy\\&=1-\frac{\lambda_{m,\mathrm{E}}\,e^{-\gamma_{\mathrm{th}}\lambda_{n,\mathrm{E}}}}{\gamma_{\mathrm{th}}\lambda_{n,\mathrm{E}}+\lambda_{m,\mathrm{E}}}.\end{aligned}$$

2) Optimal selection with preset jammer: According to this protocol, the control unit preselects a node J to act as a jammer and then employs optimal selection on the remaining nodes for each coded packet transmission. The identification of a suitable jammer could depend on the average quality of the link between the jammer and the destination. Due to space limitations, the selection process of the preset jammer is not further discussed in this paper because it does not affect the outage analysis of this protocol. As in the case of optimal selection, a node is selected to act as a relay such that

$$n^*=\arg\max_{n\in\mathcal{S}_{\mathrm{N}}\setminus J}\left(\frac{\gamma_{n,\mathrm{D}}}{\gamma_{n,\mathrm{E}}}\right).$$

Owing to the interference noise generated by J, the SINR at the destination and the SINR at the eavesdropper are given by

$$\mathrm{SINR}_{n^*,\mathrm{D}}=\frac{\gamma_{n^*,\mathrm{D}}}{\gamma_{J,\mathrm{D}}+1}$$

$$\mathrm{SINR}_{n^*,\mathrm{E}}=\frac{\gamma_{n^*,\mathrm{E}}}{\gamma_{J,\mathrm{E}}+1}.$$

Using the law of total probability, as in the previous cases, the outage probability at the destination can be expressed as:

$$\rho_{\mathrm{D}}=\sum_{n=1}^{N-1}\Pr\left[(n^*=n)\bigcap\left(\frac{\gamma_{n,\mathrm{D}}}{\gamma_{J,\mathrm{D}}+1}\leq\gamma_{\mathrm{th}}\right)\right].\qquad(14)$$

The probability that the selected relay n^* will be a particular node n can be obtained from (8) if the remaining $N-1$ of the N nodes in $\mathcal{S}_N$ are considered, that is,

$$\Pr(n^*=n)=\int_0^{\infty}\int_0^{\infty}\hat{I}_1(x,y)f_{\gamma_{n,\mathrm{D}}}(x)f_{\gamma_{n,\mathrm{E}}}(y)\,dx\,dy\qquad(15)$$

where

$$\hat{I}_1(x,y)=1-\sum_{\substack{i=1\\ i\neq n}}^{N-1}\frac{\Theta_i y}{x\Lambda_i+y}.$$

Integrating (15) over all valid values of $\gamma_{n,\mathrm{D}}$ and $\gamma_{J,\mathrm{D}}$, as dictated by (14), gives:

$$\rho_{\mathrm{D}}=\sum_{n=1}^{N-1}\int_0^{\infty}\int_0^{\infty}\int_0^{\upsilon}\hat{I}_1(x,y)f_{\gamma_{n,\mathrm{D}}}(x)f_{\gamma_{J,\mathrm{D}}}(z)f_{\gamma_{n,\mathrm{E}}}(y)\,dx\,dz\,dy$$

where $\upsilon=(z+1)\gamma_{\mathrm{th}}$. Evaluating the integrals and utilizing the relationships in [37], [38] leads to:

$$\begin{aligned}\rho_{\mathrm{D}}=\sum_{n=1}^{N-1}1-\frac{\lambda_{J,\mathrm{D}}e^{-\gamma_{\mathrm{th}}\lambda_{n,\mathrm{D}}}}{\gamma_{\mathrm{th}}\lambda_{n,\mathrm{E}}+\lambda_{J,\mathrm{D}}}+\sum_{j\neq n}^{N-1}\Theta_j\frac{\lambda_{n,\mathrm{D}}\lambda_{n,\mathrm{E}}}{\Lambda_j}\Big\{&\frac{e^{\lambda_{J,\mathrm{D}}}}{\alpha_3}H_{n,j}(\alpha_3,\beta_2,\eta_2)-\\&-\frac{1}{\alpha_1}H_{n,j}(\alpha_1,\beta_1,\eta_1)-\frac{1}{\alpha_1^2}\left[\ln\left(\frac{\lambda_{n,\mathrm{E}}}{\beta_1}\right)-\frac{\alpha_1}{\lambda_{n,\mathrm{E}}}\right]\Big\}\end{aligned}$$

with

$$H_{n,j}(\alpha,\beta,\eta)=e^{\frac{\alpha\eta}{\beta}}\left(\tfrac{1}{\alpha}-\tfrac{\eta}{\beta}\right)\mathrm{E}_1\left(\tfrac{\alpha+\beta}{\beta}\eta\right)-\tfrac{1}{\alpha}\mathrm{E}_1(\eta)+\tfrac{1}{\alpha+\beta}e^{-\eta}$$

where $\alpha_3=\alpha_1-\frac{\lambda_{j,\mathrm{D}}}{\gamma_{\mathrm{th}}\Lambda_j}$, $\beta_2=\beta_1+\frac{\lambda_{J,\mathrm{D}}}{\gamma_{\mathrm{th}}\Lambda_j}$, $\eta_1=\gamma_{\mathrm{th}}\lambda_{n,\mathrm{D}}$ and $\eta_2=\eta_1+\lambda_{J,\mathrm{D}}$.

Similarly, the outage probability at the eavesdropper can be written as:

$$\rho_{\mathrm{E}}=\sum_{n=1}^{N-1}\Pr\left[(n^*=n)\bigcap\left(\frac{\gamma_{n,\mathrm{E}}}{\gamma_{J,\mathrm{E}}+1}\leq\gamma_{\mathrm{th}}\right)\right].\qquad(16)$$

Using (15), the joint probability in (16) can be obtained from

$$\Pr\left[(n^*=n)\bigcap\left(\frac{\gamma_{n,\mathrm{E}}}{\gamma_{J,\mathrm{E}}+1}\le\gamma_{\mathrm{th}}\right)\right]=\int_0^\infty\int_0^v\int_0^\infty \hat{I}_1(x,y)f_{\gamma_{n,\mathrm{D}}}(x)\cdot \cdot f_{\gamma_{n,\mathrm{E}}}(y)f_{\gamma_{J,\mathrm{E}}}(z)\,dx\,dy\,dz$$

which allows us to rewrite (16) as:

$$\rho_{\mathrm{E}}=\sum_{n=1}^{N-1}\int_0^\infty\int_0^v\int_0^\infty \hat{I}_1(x,y)f_{\gamma_{n,\mathrm{D}}}(x)f_{\gamma_{n,\mathrm{E}}}(y)f_{\gamma_{J,\mathrm{E}}}(z)\,dx\,dy\,dz.$$

Taking into account the formulas in [37], [38], we obtain the following expression for the outage probability at the eavesdropper:

$$\begin{aligned}\rho_{\mathrm{E}}=\sum_{n=1}^{N-1}1-\frac{\lambda_{J,\mathrm{E}}e^{-\gamma_{\mathrm{th}}\lambda_{n,\mathrm{E}}}}{\gamma_{\mathrm{th}}\lambda_{n,\mathrm{E}}+\lambda_{J,\mathrm{E}}}-\sum_{j\neq n}^{N-1}\Theta_j\frac{\lambda_{n,\mathrm{D}}\lambda_{n,\mathrm{E}}}{\Lambda_j\alpha_1^2}\Bigg[\mathrm{E}_1\{\lambda_{n,\mathrm{E}}\gamma_{\mathrm{th}}\}-e^{\lambda_{J,\mathrm{E}}}\\ \mathrm{E}_1(\lambda_{n,\mathrm{E}}\gamma_{\mathrm{th}}+\lambda_{J,\mathrm{E}})-e^{-\alpha_1\gamma_{\mathrm{th}}}\frac{\lambda_{J,\mathrm{E}}(1+\alpha_1\gamma_{\mathrm{th}})}{\alpha_1\gamma_{\mathrm{th}}+\lambda_{J,\mathrm{E}}}\Bigg\{\mathrm{E}_1(\beta_1\gamma_{\mathrm{th}})\\ -e^{(\alpha_1\gamma_{\mathrm{th}}+\lambda_{J,\mathrm{E}})}\mathrm{E}_1(\lambda_{n,\mathrm{E}}\gamma_{\mathrm{th}}+\lambda_{J,\mathrm{E}})\Bigg\}+\frac{e^{-\alpha_1\gamma_{\mathrm{th}}}\lambda_{J,\mathrm{E}}\alpha_1\gamma_{\mathrm{th}}}{\alpha_4}\\ H_{n,j}(\alpha_4,\beta_3,\eta_3)+\frac{\alpha_1\lambda_{J,\mathrm{E}}e^{-\lambda_{n,\mathrm{E}}\gamma_{\mathrm{th}}}}{\lambda_{n,\mathrm{E}}\{\gamma_{\mathrm{th}}\lambda_{n,\mathrm{E}}+\lambda_{J,\mathrm{E}}\}}+\ln\left(\frac{\lambda_{n,\mathrm{E}}}{\beta_1}\right)-\frac{\alpha_1}{\lambda_{n,\mathrm{E}}}\Bigg]\end{aligned}$$

where $\alpha_4=\alpha_1\gamma_{\mathrm{th}}+\lambda_{J,\mathrm{E}}$ and $\beta_3=\eta_3=\beta_1\gamma_{\mathrm{th}}$.

The expressions for ρ_{D} and ρ_{E} that were obtained in this section for the four considered protocols will be used in the following section for the evaluation of the secrecy performance of the system when the selected relay employs RLNC.

IV. Secrecy Analysis

A. Preliminaries

As mentioned in Section I, when physical-layer security over wireless fading channels is offered in the form of cooperative jamming, the secrecy outage probability is often the preferred metric for assessing the secrecy performance of the system [18], [19], [26], [27]. Bloch *et al.* [39] provide an excellent overview of important notions of physical-layer security and present information-theoretic metrics. However, information-theoretic metrics assume *strong* security, that is, the eavesdropper decoding the encoded message is as likely as guessing the message itself. In practice, the secrecy requirements can be less stringent and alternative metrics have been proposed in [40].

Secure transmission on a multicast or broadcast network can be guaranteed if RLNC is used to combine data packets with random keys [41]. In conventional RLNC for multicast or broadcast applications, as in this paper, data packets are combined with other data packets in order to increase capacity or improve reliability without the need for retransmissions. As shown in [42], conventional RLNC can still offer strong security, if the entries of the decoding matrix are transmitted through a secure private channel to the intended destination, and source coding ensures that the zero element is not included in the data packets. Otherwise, RLNC offers *weak security*, as defined in [43], implying that a receiver (either D or E) may not be able to recover any meaningful information about the message without collecting a sufficient number of linearly independent coded packets. However, both [43] and [44] agree that strong security can be achieved if RLNC operations are over a large finite field.

The goal of this section is to investigate the inherent secrecy of RLNC for any field size, when jamming may or may not be available at the physical layer. In scenarios where secrecy requirements are not stringent, the communication process is deemed to be secure when the destination recovers the message while the eavesdropper is unable to recover even parts of the message *without guessing*. As explained in Section II, the probability of the eavesdropper being successful in recovering at least τ of the K data packets using Gaussian elimination shall be referred to as the τ-intercept probability. A variant of this metric has been used in the *algebraic security criterion* [44]. According to [44, Definition 1], the level of security provided by RLNC is a function of the data packets composing the transmitted message, the number of linearly independent coded packets collected by the eavesdropper and the number of data packets that can be recovered by Gaussian elimination. The latter quantity is actually τ and its value is assumed to be readily available in [44], i.e., the level of security can be calculated only after Gaussian elimination for a given set of collected coded packets has been performed. By contrast, we derive the probability that τ will take a specific value.

The remainder of this section presents a framework for the calculation of the τ-intercept probability and the characterization of the secrecy performance of the system.

B. Derivation of the τ-intercept probability

A receiver is required to collect K linearly independent coded packets to recover the K data packets that compose the message. The probability of recovering the message can be obtained by [45]:

$$P(K,n_{\mathrm{R}})=\prod_{i=0}^{K-1}\left[1-q^{-(n_{\mathrm{R}}-i)}\right]$$

where n_{R} is the number of received coded packets and q represents the size of the finite field over which arithmetic operations are performed. The system of linear equations, which is represented by the decoding matrix, may be partially solved using the Gaussian elimination method and τ of the K data packets could be revealed based on a subset of $r\le K$ linearly independent coded packets that have been received. The probability of recovering *exactly* $\tau\le r$ data packets, given that r linearly independent coded packets have been collected, can be obtained from [46] as follows:

$$P(\tau,K|r)=\frac{\binom{K}{\tau}}{\left[\begin{smallmatrix}K\\ r\end{smallmatrix}\right]_q}\sum_{j=0}^{K-\tau}(-1)^j\binom{K-\tau}{j}\left[\begin{smallmatrix}K-\tau-j\\ r-\tau-j\end{smallmatrix}\right]_q$$

where $\left[\begin{smallmatrix}u\\ \nu\end{smallmatrix}\right]_q$ denotes the q-binomial coefficient defined as [47]

$$\left[\begin{smallmatrix}u\\ \nu\end{smallmatrix}\right]_q=\begin{cases}\prod_{i=0}^{\nu-1}\frac{(q^u-q^i)}{(q^\nu-q^i)}, & \text{for } \nu\le u\\ 0, & \text{for } \nu>u.\end{cases}$$

Therefore, the probability of recovering *at least* τ data packets can be obtained from:

$$\mathbb{P}(\tau, n_{\mathrm{R}}) = \sum_{r=\tau}^{\min(n_{\mathrm{R}},K)} \sum_{i=\tau}^{r} P(i,K|r) P_r(K, n_{\mathrm{R}})$$

where $P_r(K, n_{\mathrm{R}})$ is the probability that r out of the n_R received coded packets are linearly independent and is given by [48, Theorem 4]

$$P_r(K, n_{\mathrm{R}}) = \frac{1}{q^{n_{\mathrm{R}}K}} \begin{bmatrix} n_{\mathrm{R}} \\ r \end{bmatrix}_q \prod_{i=0}^{r-1} (q^K - q^i).$$

Using the aforementioned expressions, we can characterize the secrecy performance of the system. Let X_{D} and X_{E} be two random variables, representing the number of transmissions required by the destination D and the eavesdropper E, respectively, such that D can recover the entire message and E can recover at least τ data packets. The cumulative distribution function of X_{D} and X_{E} can be defined as:

$$\begin{aligned} F_{\mathrm{D}}(n_{\mathrm{T}}) &= \Pr\{X_{\mathrm{D}} \le n_{\mathrm{T}}\} \\ &= \sum_{n_{\mathrm{R}}=K}^{n_{\mathrm{T}}} \binom{n_{\mathrm{T}}}{n_{\mathrm{R}}} \rho_{\mathrm{D}}^{n_{\mathrm{T}}-n_{\mathrm{R}}} (1-\rho_{\mathrm{D}})^{n_{\mathrm{R}}} \; P(K, n_{\mathrm{R}}) \end{aligned}$$

$$\begin{aligned} F_{\mathrm{E}}(\tau, n_{\mathrm{T}}) &= \Pr\{X_{\mathrm{E}} \le n_{\mathrm{T}}\} \\ &= \sum_{n_{\mathrm{R}}=\tau}^{n_{\mathrm{T}}} \binom{n_{\mathrm{T}}}{n_{\mathrm{R}}} \rho_{\mathrm{E}}^{n_{\mathrm{T}}-n_{\mathrm{R}}} (1-\rho_{\mathrm{E}})^{n_{\mathrm{R}}} \mathbb{P}(\tau, n_{\mathrm{R}}) \end{aligned}$$

where ρ_{D} and ρ_{E} represent the probability that a transmitted coded packet will not be received by the destination and the eavesdropper, respectively. Both ρ_{D} and ρ_{E} can be evaluated using the outage probability expressions that have been derived in Section III for each relay selection protocol. Essentially, $F_{\mathrm{D}}(n_{\mathrm{T}})$ is the probability that the destination will reconstruct the entire confidential message, and $F_{\mathrm{E}}(\tau, n_{\mathrm{T}})$ is the probability that the eavesdropper will recover at least τ of the K data packets that compose the message, for n_{T} *or fewer* coded packet transmissions. The respective decoding probabilities for *exactly* n_{T} coded packet transmissions can be obtained from the probability mass functions, as follows:

$$\begin{aligned} f_{\mathrm{D}}(n_{\mathrm{T}}) &= \Pr\{X_{\mathrm{D}} = n_{\mathrm{T}}\} \\ &= \begin{cases} F_{\mathrm{D}}(n_{\mathrm{T}}) - F_{\mathrm{D}}(n_{\mathrm{T}}-1), & \text{if } K < n_{\mathrm{T}} \le N_{\mathrm{T}} \\ F_{\mathrm{D}}(K), & \text{if } n_{\mathrm{T}} = K \end{cases} \end{aligned}$$

$$\begin{aligned} f_{\mathrm{E}}(n_{\mathrm{T}}) &= \Pr\{X_{\mathrm{E}} = n_{\mathrm{T}}\} \\ &= \begin{cases} F_{\mathrm{E}}(\tau, n_{\mathrm{T}}) - F_{\mathrm{E}}(\tau, n_{\mathrm{T}}-1), & \text{if } \tau < n_{\mathrm{T}} \le N_{\mathrm{T}} \\ F_{\mathrm{E}}(\tau, n_{\mathrm{T}}), & \text{if } n_{\mathrm{T}} = \tau \end{cases} \end{aligned}$$

where N_{T} represents the maximum permitted number of coded packet transmissions. In the event of the destination reconstructing the entire message before the deadline is reached, a feedback link is used to notify the control unit that additional coded packet transmissions are not required. Following the same line of reasoning as in [21], the τ-intercept probability assumes the form:

$$P_{\mathrm{int}}(\tau, N_{\mathrm{T}}) = F_{\mathrm{E}}(\tau, N_{\mathrm{T}}) \left[1 - F_{\mathrm{D}}(N_{\mathrm{T}})\right] + \sum_{n_{\mathrm{T}}=K}^{N_{\mathrm{T}}} f_{\mathrm{D}}(n_{\mathrm{T}}) \, F_{\mathrm{E}}(\tau, n_{\mathrm{T}}). \tag{17}$$

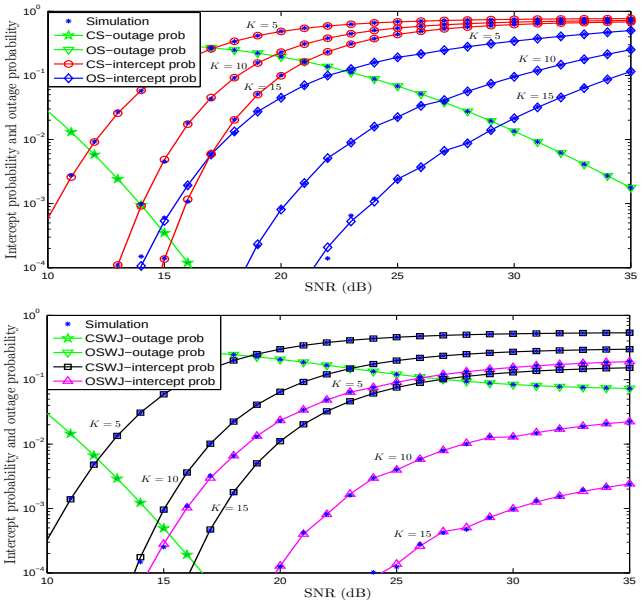

Figure 2. Comparison between simulation and theoretical results, and secrecy-reliability performance of the considered protocols for different values of K, when $q = 2$ and $\tau/K = 0.6$.

The first term in (17) is the probability that the eavesdropper will be successful in recovering at least τ data packets from the intercepted coded packets but the destination will fail to reconstruct the message after N_{T} coded packet transmissions. The second term represents the probability that the destination will recover the entire message after the n_{T}-th coded packet has been transmitted but the eavesdropper has already recovered at least τ data packets by that time.

The impact of the relay selection protocol on the outage probabilities ρ_{D} and ρ_{E}, and their effect on the intercept probability $P_{\mathrm{int}}(\tau, N_{\mathrm{T}})$ and the decoding probability at the destination $F_{\mathrm{D}}(N_{\mathrm{T}})$ will be explored in the following section.

V. Results and Discussion

This section presents simulation results and compares them with analytical results in order to validate the accuracy of the derived expressions. The secrecy performance of the system, which is reflected by the intercept probability at the eavesdropper, and the reliability performance of the system, which is associated with the outage probability of the link between the selected relay and the destination but also the decoding probability at the destination, are also discussed.

A Monte Carlo simulation platform representing the system model was developed in MATLAB. Instances where the eavesdropper successfully recovered at least τ data packets were counted and averaged over 10^4 realizations to compute the τ-intercept probability. The simulation environment considers $N = 10$ relays. Let the pair $(d_{i,\mathrm{D}}, d_{i,\mathrm{E}})$ specify the distance of node i from the destination D and the eavesdropper E, for $i = 1, \ldots, 10$. The distance pairs in the simulation environment have been configured as follows: $(2, 2.3)$, $(3, 2)$, $(4, 6)$, $(3, 4)$, $(4, 5)$, $(1, 2)$, $(1, 2.1)$, $(1.3, 1.5)$, $(1.2, 1.9)$ and $(6, 6)$. In the case of optimal selection with preset jammer, we have configured the node with distance pair $(6, 6)$ to always act as a

jammer. This node is equidistant from the destination and the eavesdropper, hence it causes the same levels of interference, on average, to both receivers. Pre-selection of this jammer yields a particular trade-off between secrecy performance and reliability but other schemes that trade reliability for secrecy are also available, e.g., [18], [27]. In all cases, the path loss exponents have been set to $\alpha_{i,j} = \alpha = 3$. Unless otherwise stated, the transmission scheme is uncoded BPSK, which is characterized by the SNR threshold $\gamma_{\text{th}} = 5.89$ dB. As explained in Section III, the outage probability depends on the relay selection protocol and the transmission scheme but not on the RLNC parameters. The lowest number of transmitted coded packets, for which the destination can decode the entire message with 90% probability or greater, has been used in the measurement of the intercept probability. Equivalently, the theoretical value of $P_{\text{int}}(\tau, N_{\text{T}})$ has been calculated from (17) for the smallest value of N_{T} that yields $F_{\text{D}}(N_{\text{T}}) \geq 0.90$. For simplicity, we assume that all nodes, including the jammer, transmit the same power, i.e. $P_i = P$. The term 'SNR' is used to refer to the ratio P/N_0, as defined in Section II. The four relay selection protocols, namely conventional selection, optimal selection, conventional selection with jammer and optimal selection with preset jammer, have been abbreviated to 'CS', 'OS', 'CSWJ' and 'OSWJ', respectively.

Fig. 2 demonstrates the agreement between simulation and analytical results, which confirms the correctness of our derivations. It also illustrates the effect of the transmitted SNR on the outage probability at the destination and compares the intercept probability of the four considered protocols. As expected, the CS scheme outperforms the other protocols in terms of reliable communication because it achieves the lowest outage probability. By contract, the CS protocol exhibits the worst performance in terms of secrecy. This is due to the fact that the CS protocol only considers the quality of relay-to-destination channels but does not take into account the relay-to-eavesdropper channels. For this reason, the OS and CSWJ protocols offer better secrecy performance than CS at the expense of reduced reliability. It can be noticed that the secrecy performance of both the CS and OS protocols deteriorates markedly at high SNR values because the intercept probability converges to one. On the other hand, the secrecy performance of the CSWJ and OSWJ protocols reveals that a jammer introduces a 'ceiling' to the intercept probability and, thus, a level of secrecy can be offered even at high SNR values. Fig. 2 also demonstrates that the secrecy-reliability tradeoff can be further improved if the message to be transmitted is segmented into a larger number of shorter data packets, that is, the value of K in RLNC is increased.

Fig. 3 investigates the effect that the field size q in RLNC has on the probability that the eavesdropper will reconstruct at least $\tau = 8$ data packets from the intercepted coded packets, for different SNR values, when $K = 15$ and either CSWJ or OSWJ is used. The figure shows that when the field size increases from $q = 2$ to $q = 4$, the intercept probability decreases notably. This is due to the fact that the larger the finite field is, the higher the probability of the received coded packets being linearly independent is. Consequently, if $q = 4$, the destination is required to collect fewer coded packets in order to reconstruct the entire message than if $q = 2$. On the other hand, if the finite field is large and the rank of the decoding matrix is smaller than K, the probability of partially reconstructing the transmitted message reduces significantly. For this reason, the fewer the linearly independent coded packets intercepted by the eavesdropper are, the smaller the probability of the eavesdropper recovering even a fraction of the message is. Fig. 2 and Fig. 3 reveal the impact of the number of data packets K and the field size q on both reliability and security. Although the intercept probability decreases if the message is segmented into a larger number of data packets or if a larger field size is used, the values of K and q cannot increase unboundedly in practice. An increase in K or q also increases the overhead of RLNC and the decoding complexity of Gaussian elimination. Upper bounds for K and q due to practical limitations are discussed in [49].

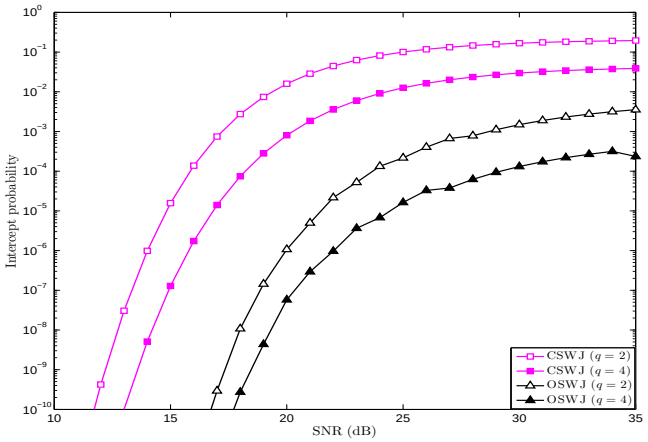

Figure 3. Effect of the field size q on the secrecy performance of both CSWJ and OSWJ, as a function of the SNR, when $\tau = 8$ and $K = 15$.

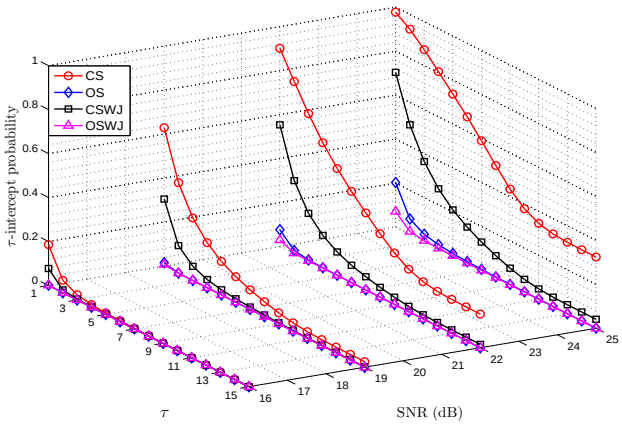

Figure 4. Performance comparison in terms of the amount of recovered data and the SNR value, for $q = 2$ and $K = 15$.

Fig. 4 compares the τ-intercept probability offered by the considered protocols for all possible values of τ and different transmitted SNR values, when $q = 2$ and $K = 15$. At low SNR values, the probability of recovering data packets from intercepted coded packets is very small, regardless of the adopted protocol. For example, even when the CS protocol is employed, the probability of the eavesdropper recovering

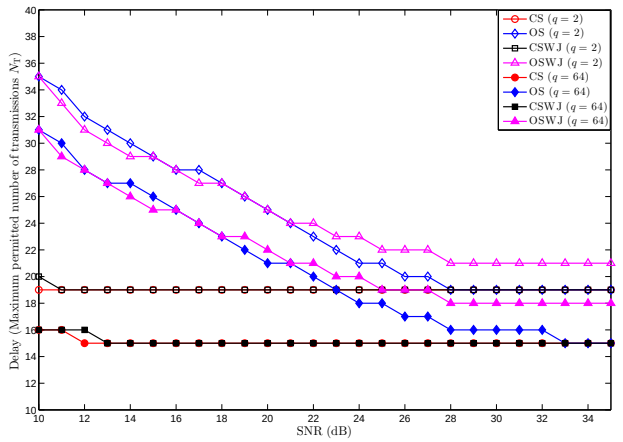

Figure 5. Delay performance as a function of SNR for $q = 2$ and $q = 64$, when $K = 15$ is considered.

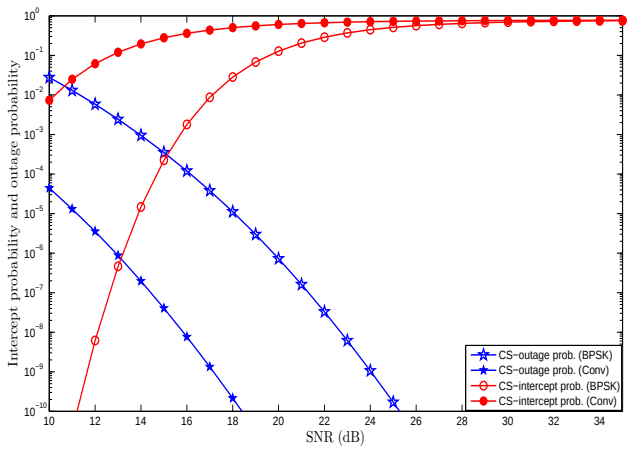

Figure 6. Secrecy-reliability trade-off as a function of the SNR for two different transmission schemes, $K = 15$, $q = 2$ and $\tau = 8$.

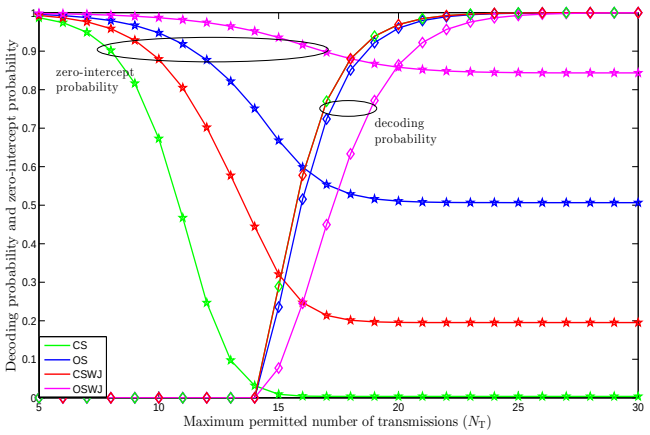

Figure 7. Performance comparison based on the decoding probability and the zero-intercept probability at SNR=30 dB, for $K = 15$ and $q = 2$.

at least one data packet ($\tau = 1$) is 0.18 at SNR $= 16$ dB. However, for high SNR values, the CS scheme clearly yields the worst performance. For example, the performance curve of the CS protocol shows that even though the probability of recovering the entire data message ($\tau = 15$) is low, the eavesdropper can still recover a large portion of data with high probability. The other three protocols provide better performance even for $\tau = 1$.

Fig. 5 compares the delay performance of each protocol, in terms of the maximum permitted number of coded packet transmissions required by the destination to recover the entire data message. This delay metric also reflects the reliability of the network. The impact of the field size q on the secrecy-reliability tradeoff is depicted in this figure too. Both CS and CSWJ exhibit fixed and similar delay performance in the high SNR regime, even though CS offers higher link reliability than CSWJ, as established in Fig. 2. For $q = 64$, both CS and CSWJ achieve the minimum delay performance, i.e. $N_T = 15$. The worst-case delay is experienced when RLNC over fields of size $q = 2$ is combined with either OS or OSWJ. The delay of OS and OSWJ is reduced if the field size is increased to $q = 64$ and approaches the delay of CS and CSWJ for an increasing SNR value.

Fig. 6 focuses on the CS scheme and further investigates the reliability versus secrecy trade-off between uncoded BPSK and coded BPSK. The SNR threshold for coded BPSK, which employs convolutional coding, is set to $\gamma_{th} = -0.983$ dB, as mentioned in Section III. As expected, coded BPSK achieves a lower outage probability than uncoded BPSK at the expense of a notably higher intercept probability. This is due to the fact that the information redundancy introduced by convolutional coding assists not only the destination but also the eavesdropper in the error-free reception of coded packets and the recovery of at least τ data packets. Our proposed framework can thus be used to identify modulation and coding schemes that offer a required balance between security and reliability.

For each point depicted in the previous figures, the maximum permitted number of transmitted coded packets N_T has been computed so that the probability of the destination decoding the entire message is at least 90%, i.e., $F_D(N_T) \geq 0.9$. In contrast, Fig. 7 investigates the impact of N_T on both the decoding probability at the destination $F_D(N_T)$ and the probability that the eavesdropper will be unable to recover any data packets. The latter probability is referred to as the *zero-intercept probability* and is given by $1 - P_{int}(1, N_T)$. As expected, an increase in coded packet transmissions improves the decoding probability at the destination and decreases the zero-intercept probability. The benefit from using a feedback link to notify the control unit to cease the transmission of coded packets when the destination has recovered the entire message, can also be observed in Fig. 7. For a high value of N_T, the destination is more likely to decode the message when fewer than N_T coded packets have been transmitted. As a result, the transmission process will be terminated earlier than anticipated and the eavesdropper will be unable to collect more coded packets. For this reason, the zero-intercept probability gradually converges to a fixed value for an increasing value of N_T. We note that the CS protocol yields the highest decoding probability but provides no guarantees that the eavesdropper will recover no data packets. The selection of a jammer that causes the least interference to the transmitting relay gives CSWJ a security advantage over CS without a compromise on

the decoding probability. Exploitation of the eavesdropper's CSI can further increase the zero-intercept probability and boost security, even when a jammer is not employed, as demonstrated by the OS protocol. On the other hand, OSWJ yields the highest zero-intercept probability at the expense of a lower decoding probability than the other protocols. The results reaffirm that the security advantage gained by opting for a protocol other than CS clearly outweighs the loss in reliability, when $\mathrm{SNR} = 30$ dB.

VI. Conclusion

In order to address the vulnerability of wireless communication networks against eavesdropping attacks, we developed a framework that combines random linear network coding at the application layer and physical-layer security in the form of relay selection with or without cooperative jamming. Four relay selection protocols were considered and analytical expressions of the outage probability at the intended destination and the eavesdropper were derived. In order to quantify the amount of information leakage to the eavesdropper, a novel metric called τ-intercept probability was proposed. This metric, which utilizes the outage probabilities associated to each relay selection protocol, provides a measure of security that is jointly offered by the application and physical layers in scenarios where secrecy requirements are not stringent. Our analysis demonstrated that relay selection based on both the eavesdropper's CSI and the destination's CSI achieves a good balance between security and reliability, when a jammer is not employed. If a jammer is used, reliability can be traded for security. On the other hand, if the eavesdropper's CSI is not available, the selection of a relay and a jammer based solely on the destination's CSI favors reliability, while still providing some secrecy guarantees. We also noted that the field size over which random linear network coding is performed at the application layer as well as the adopted modulation and coding scheme at the physical layer can be modified to fine-tune the trade-off between security and reliability.

Future directions on this topic could involve the introduction of direct communication from the source to both the destination and the eavesdropper, the consideration of multiple eavesdroppers and the study of the effect of constellation rotation, as proposed in [22], on the security and reliability of the network.

References

[1] V. Ç. Güngör and G. P. Hancke, "Industrial wireless sensor networks: Challenges, design principles, and technical approaches," *IEEE Trans. Ind. Electron.*, vol. 56, no. 10, pp. 4258–4265, Oct. 2009.

[2] W. Jiang, T. Kaiser, and A. J. H. Vinck, "A robust opportunistic relaying strategy for co-operative wireless communications," *IEEE Trans. Wireless Commun.*, vol. 15, no. 4, pp. 2642–2655, Apr. 2016.

[3] A. Bletsas, A. Khisti, D. P. Reed, and A. Lippman, "A simple cooperative diversity method based on network path selection," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 3, pp. 659–672, Mar. 2006.

[4] J. Luo, J. Hu, D. Wu, and R. Li, "Opportunistic routing algorithm for relay node selection in wireless sensor networks," *IEEE Trans. Ind. Informat.*, vol. 11, no. 1, pp. 112–121, Feb. 2015.

[5] R. Madan, N. B. Mehta, A. F. Molisch, and J. Zhang, "Energy-efficient cooperative relaying over fading channels with simple relay selection," *IEEE Trans. Wireless Commun.*, vol. 7, no. 8, pp. 3013–3025, Aug. 2008.

[6] J. Niu, L. Cheng, Y. Gu, L. Shu, and S. K. Das, "R3E: Reliable reactive routing enhancement for wireless sensor networks," *IEEE Trans. Ind. Informat.*, vol. 10, no. 1, pp. 784–794, Feb. 2014.

[7] Z. Iqbal, K. Kim, and H. N. Lee, "A cooperative wireless sensor network for indoor industrial monitoring," *IEEE Trans. Ind. Informat.*, vol. 13, no. 2, pp. 482–491, Apr. 2017.

[8] N. Marchenko, T. Andre, G. Brandner, W. Masood, and C. Bettstetter, "An experimental study of selective cooperative relaying in industrial wireless sensor networks," *IEEE Trans. Ind. Informat.*, vol. 10, no. 3, pp. 1806–1816, Aug. 2014.

[9] T. Ho, M. Médard, R. Koetter, D. R. Karger, M. Effros, J. Shi, and B. Leong, "A random linear network coding approach to multicast," *IEEE Trans. Inf. Theory*, vol. 52, no. 10, pp. 4413–4430, Oct. 2006.

[10] S. Deb, M. Effros, T. Ho, D. R. Karger, R. Koetter, D. S. Lun, M. Médard, and N. Ratnakar, "Network coding for wireless applications: A brief tutorial," in *Proc. Int. Workshop on Wireless Ad Hoc Networks*, London, UK, May 2005.

[11] D. Szabo, A. Gulyas, F. H. P. Fitzek, and D. E. Lucani, "Towards the tactile internet: Decreasing communication latency with network coding and software defined networking," in *Proc. 21st European Wireless Conf.*, Budapest, Hungary, May 2015.

[12] Q. F. Zhou, Y. Li, F. C. Lau, and B. Vucetic, "Decode-and-forward two-way relaying with network coding and opportunistic relay selection," *IEEE Trans. Commun.*, vol. 58, no. 11, pp. 3070–3076, Nov. 2010.

[13] X. D. Jia, L. X. Yang, H. Y. Fu, B. M. Feng, and Y. F. Qi, "Two-way denoise-and-forward network coding opportunistic relaying with jointing adaptive modulation relay selection criterions," *IET Communications*, vol. 6, no. 2, pp. 194–202, Jan. 2012.

[14] Q. You, Y. Li, and Z. Chen, "Joint relay selection and network coding for error-prone two-way decode-and-forward relay networks," *IEEE Trans. Commun.*, vol. 62, no. 10, pp. 3420–3433, Oct. 2014.

[15] I. Krikidis, "Opportunistic relay selection for cooperative networks with secrecy constraints," *IET Communications*, vol. 4, no. 15, pp. 1787–1791, Oct. 2010.

[16] V. N. Q. Bao, N. Linh-Trung, and M. Debbah, "Relay selection schemes for dual-hop networks under security constraints with multiple eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 12, no. 12, pp. 6076–6085, Dec. 2013.

[17] J. Zhu, Y. Zou, B. Champagne, W. P. Zhu, and L. Hanzo, "Security-reliability tradeoff analysis of multirelay-aided decode-and-forward cooperation systems," *IEEE Trans. Veh. Technol.*, vol. 65, no. 7, pp. 5825–5831, Jul. 2016.

[18] I. Krikidis, J. S. Thompson, and S. Mclaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Trans. Wireless Commun.*, vol. 8, no. 10, pp. 5003–5011, Oct. 2009.

[19] L. Wang, Y. Cai, Y. Zou, W. Yang, and L. Hanzo, "Joint relay and jammer selection improves the physical layer security in the face of CSI feedback delays," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6259–6274, Aug. 2016.

[20] N. Cai and R. W. Yeung, "Secure network coding," in *Proc. IEEE Int. Symp. on Inform. Theory (ISIT)*, Lausanne, Switzerland, Jun. 2002.

[21] A. S. Khan, A. Tassi, and I. Chatzigeorgiou, "Rethinking the intercept probability of random linear network coding," *IEEE Commun. Lett.*, vol. 19, no. 10, pp. 1762–1765, Oct. 2015.

[22] L. Sun, P. Ren, Q. Du, and Y. Wang, "Fountain-coding aided strategy for secure cooperative transmission in industrial wireless sensor networks," *IEEE Trans. Ind. Informat.*, vol. 12, no. 1, pp. 291–300, Feb. 2016.

[23] K. R. Liu, *Cooperative communications and networking*. Cambridge University Press, 2009.

[24] K. B. Letaief and W. Zhang, "Cooperative communications for cognitive radio networks," *Proc. IEEE*, vol. 97, no. 5, pp. 878–893, May 2009.

[25] K. Wang, L. Yuan, T. Miyazaki, D. Zeng, S. Guo, and Y. Sun, "Strategic anti-eavesdropping game for physical layer security in wireless cooperative networks," *IEEE Trans. Commun.*, pp. 1–1, May 2017.

[26] T. M. Hoang, T. Q. Duong, N.-S. Vo, and C. Kundu, "Physical layer security in cooperative energy harvesting networks with a friendly jammer," *IEEE Commun. Lett.*, vol. 6, no. 2, pp. 174–177, Apr. 2017.

[27] D. H. Ibrahim, E. S. Hassan, and S. A. El-Doli, "Relay and jammer selection schemes for improving physical layer security in two-way cooperative networks," *Computers & Security*, vol. 50, pp. 47–59, May 2015.

[28] Y. Zou, X. Wang, and W. Shen, "Physical-layer security with multiuser scheduling in cognitive radio networks," *IEEE Trans. Commun.*, vol. 61, no. 12, pp. 5103–5113, Dec. 2013.

[29] A. Mukherjee and A. L. Swindlehurst, "Detecting passive eavesdroppers in the MIMO wiretap channel," in *Proc. IEEE Int. Conf. Acoustics, Speech and Sign. Proc. (ICASSP)*, Kyoto, Japan, Mar. 2012.

[30] I. Chatzigeorgiou, I. J. Wassell, and R. Carrasco, "On the frame error rate of transmission schemes on quasi-static fading channels," in *Proc. 42nd Conf. on Inform. Sciences and Systems (CISS)*, Princeton, USA, Mar. 2008, pp. 577–581.

[31] Y. Xi, A. Burr, J. Wei, and D. Grace, "A general upper bound to evaluate packet error rate over quasi-static fading channels," *IEEE Trans. Wireless Commun.*, vol. 10, no. 5, pp. 1373–1377, May 2011.

[32] T. Liu, Y. Li, Q. Huo, and B. Jiao, "Performance analysis of hybrid relay selection in cooperative wireless systems," *IEEE Trans. Commun.*, vol. 60, no. 3, pp. 779–788, Mar. 2012.

[33] A. Goldsmith, *Wireless communications*. Cambridge University Press, 2005.

[34] H. Niu, M. Iwai, K. Sezaki, L. Sun, and Q. Du, "Exploiting fountain codes for secure wireless delivery," *IEEE Commun. Lett.*, vol. 18, no. 5, pp. 777–780, May 2014.

[35] A. Papoulis and S. U. Pillai, *Probability, random variables, and stochastic processes*. McGraw-Hill Education, 2002.

[36] A. Bletsas, A. G. Dimitriou, and J. N. Sahalos, "Interference-limited opportunistic relaying with reactive sensing," *IEEE Trans. Wireless Commun.*, vol. 9, no. 1, pp. 14–20, Jan. 2010.

[37] A. Jeffrey and D. Zwillinger, *Table of integrals, series, and products*. Academic Press, 2007.

[38] M. Geller and E. W. Ng, "A table of integrals of the exponential integral," *Journal of Research of the National Bureau of Standards*, vol. 71, pp. 1–20, 1969.

[39] M. Bloch, M. Hayashi, and A. Thangaraj, "Error-control coding for physical-layer secrecy," *Proc. IEEE*, vol. 103, no. 10, pp. 1725–1746, Oct. 2015.

[40] B. He, X. Zhou, and A. L. Swindlehurst, "On secrecy metrics for physical layer security over quasi-static fading channels," *IEEE Trans. Wireless Commun.*, vol. 15, no. 10, pp. 6913–6924, Oct. 2016.

[41] N. Cai and T. Chan, "Theory of secure network coding," *Proc. IEEE*, vol. 99, no. 3, pp. 421–437, Mar. 2011.

[42] L. Lima, J. P. Vilela, J. Barros, and M. Medard, "An information-theoretic cryptanalysis of network coding - Is protecting the code enough?" in *Proc. Int. Symp. on Inform. Theory and its Applications*, Dec. 2008, pp. 1–6.

[43] K. Bhattad and K. R. Narayanan, "Weakly secure network coding," in *Proc. 1st Workshop on Network Coding, Theory and Applications (NetCod)*, Riva del Garda, Italy, Apr. 2005.

[44] L. Lima, M. Médard, and J. Barros, "Random linear network coding: A free cipher?" in *Proc. IEEE Int. Symp. on Inform. Theory*, Nice, France, Jun. 2007, pp. 546–550.

[45] O. Trullols-Cruces, J. Barcelo-Ordinas, and M. Fiore, "Exact decoding probability under random linear network coding," *IEEE Commun. Lett.*, vol. 15, no. 1, pp. 67–69, Jan. 2011.

[46] J. Claridge and I. Chatzigeorgiou, "Probability of partially decoding network-coded messages," *IEEE Commun. Lett.*, vol. PP, no. 99, pp. 1–1, May 2017.

[47] P. J. Cameron, *Combinatorics: Topics, techniques, algorithms*. Cambridge University Press, 1994.

[48] È. M. Gabidulin, "Theory of codes with maximum rank distance," *Problems of Information Transmission*, vol. 21, no. 1, pp. 1–12, Jan. 1985.

[49] J. Heide, M. V. Pedersen, F. H. P. Fitzek, and M. Médard, "On code parameters and coding vector representation for practical RLNC," in *IEEE International Conference on Communications (ICC)*, Jun. 2011.